



Computer Forensics LLC
 1880 North Congress Ave, Suite 333
 Boynton Beach, Florida 33426
 Main: 561.404.3074
www.ComputerForensicsLLC.com

Reference Malibu Case Raleigh

I received FedEx package tracking number 772371638455 on 12/26/2014 from Tim Kiefer D4 Data in Rochester, NY. The package contained one Western Digital HDD (hard disk drive). The Western Digital HDD was encrypted with TrueCrypt software. I was provided the password to unencrypt the HDD. Once the HDD was unencrypted I noticed it had several folders on the drive including EnCase images of 2 hard drives listed as belong to Mr. Raleigh. The drive also contained 2 Cellebrite iPad extractions along with photographs of the devices.

Name	Date modified	Type	Size
iPad Backup	12/5/2014 12:13 PM	File folder	
iPad2	12/10/2014 10:49 ...	File folder	
JRaleigh_LT1	12/5/2014 5:31 AM	File folder	
JRaleigh_RT2	12/4/2014 9:18 PM	File folder	
901014580 JRaleigh Photos	12/10/2014 2:25 PM	Compressed (zipp...)	7,486 KB

EnCase D4 Data Imaging Summary “JRaleigh_LT1” aka “MacBook C02HW056DV31”

Name	MacBook C02HW056DV31
Actual Date	12/03/14 08:07:41PM
Target Date	12/03/14 08:07:41PM
Case Number	90-1014-580
Evidence Number	Not provided
Examiner Name	Molly Heaven-Hoyle
Notes	Not provided
Model	APPLE HDD HTS541010A9E682
Serial Number	J8200076GN56NA
Drive Type	Fixed
File Integrity	Completely Verified, 0 Errors
Acquisition MD5	23201464e479650b4a4018536c792072
Verification MD5	23201464e479650b4a4018536c792072
Acquisition SHA1	eb3a32e6fb0e95c4930e18404c2ae4b4b99972e4
Verification SHA1	eb3a32e6fb0e95c4930e18404c2ae4b4b99972e4
GUID	b9360c5362d042cb8c44a73482485d3d
Read Errors	0
Missing Sectors	0
Disk Elements	No
CRC Errors	0
Compression	Good
Total Size	1,000,204,886,016 Bytes (931.5GB)
Total Sectors	1,953,525,168
Disk Signature	00000000
Partitions	Valid



EnCase D4 Data Imaging Summary “JRaleigh_RT2” aka “MacBook 340269NBATM”

Name	MacBook 340269NBATM
Actual Date	12/03/14 04:02:13PM
Target Date	12/03/14 04:02:13PM
Case Number	90-1014-580
Evidence Number	Not provided
Examiner Name	Molly Heaven-Hoyle
Notes	Not provided
Model	Hitachi HTS545050B9A300
Serial Number	101112PBN475X7C13R1L
Drive Type	Fixed
File Integrity	Completely Verified, 0 Errors
Acquisition MD5	84b893f00da4a899568768ccb1a77729
Acquisition SHA1	05d8a75544f18968d79ffcf9e3d67e21f1db3691
Verification SHA1	05d8a75544f18968d79ffcf9e3d67e21f1db3691 cc6f062f4e9741c09d1d662845827a48
GUID	
Read Errors	0
Missing Sectors	0
Disk Elements	No
CRC Errors	0
Compression	Good
Total Size	500,107,862,016 Bytes (465.8GB)
Total Sectors	976,773,168
Disk Signature	00000000
Partitions	Valid

**JRaleigh_LT1” aka “MacBook C02HW056DV31**Time Zone Settings

JRaleigh\MacBook C02HW056DV31\D\Macintosh HD\private\etc\localtime
Configured Time Zone:America/Detroit

/usr/share/zoneinfo/America/Detroit

OS Information

ProductBuildVersion: 14B25
ProductCopyright: 1983-2014 Apple Inc.
ProductName: Mac OS X
ProductUserVisibleVersion: 10.10.1
ProductVersion: 10.10.1

User Information

	Name	File Ext	Last Accessed	File Created	Full Path
1	.localized	localized	09/09/14 06:16:34PM	09/09/14 06:16:34PM	JRaleigh\MacBook C02HW056DV31\D\Macintosh HD\Users\.localized
2	Guest		10/17/14 11:40:29AM	10/17/14 11:40:27AM	JRaleigh\MacBook C02HW056DV31\D\Macintosh HD\Users\Guest
3	jr		12/02/14 11:19:00PM	07/27/10 12:51:33AM	JRaleigh\MacBook C02HW056DV31\D\Macintosh HD\Users\jr
4	macports		07/01/12 10:28:38AM	03/01/12 10:11:52AM	JRaleigh\MacBook C02HW056DV31\D\Macintosh HD\Users\macports
5	Shared		10/17/14 10:37:15AM	06/24/11 05:49:24PM	JRaleigh\MacBook C02HW056DV31\D\Macintosh HD\Users\Shared

JRaleigh LT1" aka "MacBook C02HW056DV31 Findings:

A search of the hard drive for evidence relating to Malibu Media movies was negative. A search of the hard drive for evidence of BitTorrent use was positive as outlined in this report.

1. Using IEF (Internet Evidence Finder Software by Magnet Forensics) I located hundreds of “Cloud Services” related URLs (Web Addresses) relating to sites like Dropbox and Google Drive. Please review the final case files folder “Cloud Services URLs” for complete list.
 2. Using IEF I located several Adium, skype and chats about BitTorrent (Adium is a free instant messaging application for Mac OS X). Please review the final case files folder “Complete List Adium Chats” for complete list and for a list of just the chats pertaining to the keyword Torrent please review the folder “IEF Torrent Keyword Search Hits”.
 3. Using IEF I located several Skype & iMessage chats messages about Torrents, hacking etc. Please review the final case files folder “IEF Torrent Keyword Search Hits” for complete list.
 - 4: EnCase Screen Capture showing the related “NFO” file. NFO files are commonly associated with copyright infringement files and are often included with the infringed file(s).

The screenshot shows the EnCase Forensic interface. The top menu bar includes File, Edit, View, Tools, Help, Add Device, Search, Refresh, and Query. The main window has tabs for Cases, File Viewers, Keywords, Entries, Bookmarks, Search Hits, Records, Devices, Secure Storage, and Hash Properties. The Entries tab is selected, displaying a tree view of files under a 'Home' folder, including 'Kyle', 'Modstri IP', 'Movies', 'Hackers', 'Lost Highway 1997 720p BRRip x264 RmD (HDScene Release)', and 'MyThumbDrive'. Below the tree view is a table with columns for Name, File Ext, Last Accessed, and File Created. Two entries are listed: 'Lost Highway 1997 720p BRRip x264 RmD (HDScene Release).mkv' (mkv, 09/25/12 09:40:19PM, 09/21/12 11:54:21PM) and 'SceneUnderground.nfo' (nfo, 09/22/12 06:21:49AM, 09/22/12 12:32:03AM). The bottom half of the screen shows a hex editor with a text overlay of file metadata. The text includes release information like 'Release iNFO', 'Release Title', 'Releaser Name', 'Release Type', 'IMDB URL', 'File Size', and various comments from release groups. The hex editor shows binary data corresponding to the text.

Name	File Ext	Last Accessed	File Created
Lost Highway 1997 720p BRRip x264 RmD (HDScene Release).mkv	mkv	09/25/12 09:40:19PM	09/21/12 11:54:21PM
SceneUnderground.nfo	nfo	09/22/12 06:21:49AM	09/22/12 12:32:03AM

Text Hex Doc Transcript Picture Report Console Details Output Lock Codepage 0/7197604

1990 : Lost Highway 1997 720p BRRip x264 RmD (HDScene Release) :
2085 : :
2180 : :
2275 : :
2370 : :
2465 : :
2560 : :
2655 : Release iNFO :
2750 : :
2845 : Release Title : Lost Highway 1997 720p BRRip x264 RmD (HDScene Release) :
2940 : :
3035 : :
3130 : Releaser Name : RmD @ HDScene :
3250 : :
3260 : :
3355 : :
3450 : Release Type : H.264 :
3545 : :
3640 : :
3735 : IMDB URL : http://www.imdb.com/title/tt0116922/ :
3830 : :
3925 : :
4020 : File Size : 1.77 GB :
4115 : :
4210 : :
4305 : :
4400 : :
4494 : :
4589 : :
4684 : " +Ü GRETZ Ü + " :
4779 : :
4874 : :
4969 : DarkScene,TheSwede,Noir,TheFalcon007,blackjesus,SUDesigner,HDScene Encoders,
5064 : SceneUnderground,HD11TB,Movie-Torrentz,Torrent-Force RG,AhaShare,
5159 : 1337x,Resource ExtraTorrent RG,DDR RG,RG,BSBT RG,Atomic RG,LKRG,FLAUL3SS,3Li,
5254 : SceneU uploaders,twentyforty and all other p2p release groups out there !!! :
5349 : :
5444 : :
5539 : :
5634 : We are a new release group and searching for good encoders. So if you are Ü :
5729 : Ü interested to join, contact us at http://sceneunderground.org. Ü :
5824 : Ü Source and encoding tutorial(if necessary) will be provided. Ü :
5919 : Ü :
6014 : Ü :
6109 : :
6204 : :
6299 : :
6394 : :
6488 : :
6578 : NFO created by: TheFalcon007 :
6668 : :
6753 : :
6848 : :
6943 : :
7038 : :
7133 : :
7228 : :
7323 : :
7418 : :
7513 : :
7608 : :
7703 : :
7798 : :
7893 : :
7988 : :
8083 : :
8178 : :
8273 : :
8368 : :
8463 : :
8558 : :
8653 : :
8748 : :
8843 : :
8938 : :
9033 : :
9128 : :
9223 : :
9318 : :
9413 : :
9508 : :
9593 : :
9688 : :
9783 : :
9878 : :
9973 : :
10068 : :
10163 : :
10258 : :
10353 : :
10448 : :
10543 : :
10638 : :
10733 : :
10828 : :
10923 : :
11018 : :
11113 : :
11208 : :
11303 : :
11398 : :
11493 : :
11588 : :
11683 : :
11778 : :
11873 : :
11968 : :
12063 : :
12158 : :
12253 : :
12348 : :
12443 : :
12538 : :
12633 : :
12728 : :
12823 : :
12918 : :
13013 : :
13108 : :
13203 : :
13398 : :
13493 : :
13588 : :
13683 : :
13778 : :
13873 : :
13968 : :
14063 : :
14158 : :
14253 : :
14348 : :
14443 : :
14538 : :
14633 : :
14728 : :
14823 : :
14918 : :
15013 : :
15108 : :
15203 : :
15398 : :
15493 : :
15588 : :
15683 : :
15778 : :
15873 : :
15968 : :
16063 : :
16158 : :
16253 : :
16348 : :
16443 : :
16538 : :
16633 : :
16728 : :
16823 : :
16918 : :
17013 : :
17108 : :
17203 : :
17398 : :
17493 : :
17588 : :
17683 : :
17778 : :
17873 : :
17968 : :
18063 : :
18158 : :
18253 : :
18348 : :
18443 : :
18538 : :
18633 : :
18728 : :
18823 : :
18918 : :
19013 : :
19108 : :
19203 : :
19398 : :
19493 : :
19588 : :
19683 : :
19778 : :
19873 : :
19968 : :
20063 : :
20158 : :
20253 : :
20348 : :
20443 : :
20538 : :
20633 : :
20728 : :
20823 : :
20918 : :
21013 : :
21108 : :
21203 : :
21398 : :
21493 : :
21588 : :
21683 : :
21778 : :
21873 : :
21968 : :
22063 : :
22158 : :
22253 : :
22348 : :
22443 : :
22538 : :
22633 : :
22728 : :
22823 : :
22918 : :
23013 : :
23108 : :
23203 : :
23398 : :
23493 : :
23588 : :
23683 : :
23778 : :
23873 : :
23968 : :
24063 : :
24158 : :
24253 : :
24348 : :
24443 : :
24538 : :
24633 : :
24728 : :
24823 : :
24918 : :
25013 : :
25108 : :
25203 : :
25398 : :
25493 : :
25588 : :
25683 : :
25778 : :
25873 : :
25968 : :
26063 : :
26158 : :
26253 : :
26348 : :
26443 : :
26538 : :
26633 : :
26728 : :
26823 : :
26918 : :
27013 : :
27108 : :
27203 : :
27398 : :
27493 : :
27588 : :
27683 : :
27778 : :
27873 : :
27968 : :
28063 : :
28158 : :
28253 : :
28348 : :
28443 : :
28538 : :
28633 : :
28728 : :
28823 : :
28918 : :
29013 : :
29108 : :
29203 : :
29398 : :
29493 : :
29588 : :
29683 : :
29778 : :
29873 : :
29968 : :
30063 : :
30158 : :
30253 : :
30348 : :
30443 : :
30538 : :
30633 : :
30728 : :
30823 : :
30918 : :
31013 : :
31108 : :
31203 : :
31398 : :
31493 : :
31588 : :
31683 : :
31778 : :
31873 : :
31968 : :
32063 : :
32158 : :
32253 : :
32348 : :
32443 : :
32538 : :
32633 : :
32728 : :
32823 : :
32918 : :
33013 : :
33108 : :
33203 : :
33398 : :
33493 : :
33588 : :
33683 : :
33778 : :
33873 : :
33968 : :
34063 : :
34158 : :
34253 : :
34348 : :
34443 : :
34538 : :
34633 : :
34728 : :
34823 : :
34918 : :
35013 : :
35108 : :
35203 : :
35398 : :
35493 : :
35588 : :
35683 : :
35778 : :
35873 : :
35968 : :
36063 : :
36158 : :
36253 : :
36348 : :
36443 : :
36538 : :
36633 : :
36728 : :
36823 : :
36918 : :
37013 : :
37108 : :
37203 : :
37398 : :
37493 : :
37588 : :
37683 : :
37778 : :
37873 : :
37968 : :
38063 : :
38158 : :
38253 : :
38348 : :
38443 : :
38538 : :
38633 : :
38728 : :
38823 : :
38918 : :
39013 : :
39108 : :
39203 : :
39398 : :
39493 : :
39588 : :
39683 : :
39778 : :
39873 : :
39968 : :
40063 : :
40158 : :
40253 : :
40348 : :
40443 : :
40538 : :
40633 : :
40728 : :
40823 : :
40918 : :
41013 : :
41108 : :
41203 : :
41398 : :
41493 : :
41588 : :
41683 : :
41778 : :
41873 : :
41968 : :
42063 : :
42158 : :
42253 : :
42348 : :
42443 : :
42538 : :
42633 : :
42728 : :
42823 : :
42918 : :
43013 : :
43108 : :
43203 : :
43398 : :
43493 : :
43588 : :
43683 : :
43778 : :
43873 : :
43968 : :
44063 : :
44158 : :
44253 : :
44348 : :
44443 : :
44538 : :
44633 : :
44728 : :
44823 : :
44918 : :
45013 : :
45108 : :
45203 : :
45398 : :
45493 : :
45588 : :
45683 : :
45778 : :
45873 : :
45968 : :
46063 : :
46158 : :
46253 : :
46348 : :
46443 : :
46538 : :
46633 : :
46728 : :
46823 : :
46918 : :
47013 : :
47108 : :
47203 : :
47398 : :
47493 : :
47588 : :
47683 : :
47778 : :
47873 : :
47968 : :
48063 : :
48158 : :
48253 : :
48348 : :
48443 : :
48538 : :
48633 : :
48728 : :
48823 : :
48918 : :
49013 : :
49108 : :
49203 : :
49398 : :
49493 : :
49588 : :
49683 : :
49778 : :
49873 : :
49968 : :
50063 : :
50158 : :
50253 : :
50348 : :
50443 : :
50538 : :
50633 : :
50728 : :
50823 : :
50918 : :
51013 : :
51108 : :
51203 : :
51398 : :
51493 : :
51588 : :
51683 : :
51778 : :
51873 : :
51968 : :
52063 : :
52158 : :
52253 : :
52348 : :
52443 : :
52538 : :
52633 : :
52728 : :
52823 : :
52918 : :
53013 : :
53108 : :
53203 : :
53398 : :
53493 : :
53588 : :
53683 : :
53778 : :
53873 : :
53968 : :
54063 : :
54158 : :
54253 : :
54348 : :
54443 : :
54538 : :
54633 : :
54728 : :
54823 : :
54918 : :
55013 : :
55108 : :
55203 : :
55398 : :
55493 : :
55588 : :
55683 : :
55778 : :
55873 : :
55968 : :
56063 : :
56158 : :
56253 : :
56348 : :
56443 : :
56538 : :
56633 : :
56728 : :
56823 : :
56918 : :
57013 : :
57108 : :
57203 : :
57398 : :
57493 : :
57588 : :
57683 : :
57778 : :
57873 : :
57968 : :
58063 : :
58158 : :
58253 : :
58348 : :
58443 : :
58538 : :
58633 : :
58728 : :
58823 : :
58918 : :
59013 : :
59108 : :
59203 : :
59398 : :
59493 : :
59588 : :
59683 : :
59778 : :
59873 : :
59968 : :
60063 : :
60158 : :
60253 : :
60348 : :
60443 : :
60538 : :
60633 : :
60728 : :
60823 : :
60918 : :
61013 : :
61108 : :
61203 : :
61398 : :
61493 : :
61588 : :
61683 : :
61778 : :
61873 : :
61968 : :
62063 : :
62158 : :
62253 : :
62348 : :
62443 : :
62538 : :
62633 : :
62728 : :
62823 : :
62918 : :
63013 : :
63108 : :
63203 : :
63398 : :
63493 : :
63588 : :
63683 : :
63778 : :
63873 : :
63968 : :
64063 : :
64158 : :
64253 : :
64348 : :
64443 : :
64538 : :
64633 : :
64728 : :
64823 : :
64918 : :
65013 : :
65108 : :
65203 : :
65398 : :
65493 : :
65588 : :
65683 : :
65778 : :
65873 : :
65968 : :
66063 : :
66158 : :
66253 : :
66348 : :
66443 : :
66538 : :
66633 : :
66728 : :
66823 : :
66918 : :
67013 : :
67108 : :
67203 : :
67398 : :
67493 : :
67588 : :
67683 : :
67778 : :
67873 : :
67968 : :
68063 : :
68158 : :
68253 : :
68348 : :
68443 : :
68538 : :
68633 : :
68728 : :
68823 : :
68918 : :
69013 : :
69108 : :
69203 : :
69398 : :
69493 : :
69588 : :
69683 : :
69778 : :
69873 : :
69968 : :
70063 : :
70158 : :
70253 : :
70348 : :
70443 : :
70538 : :
70633 : :
70728 : :
70823 : :
70918 : :
71013 : :
71108 : :
71203 : :
71398 : :
71493 : :
71588 : :
71683 : :
71778 : :
71873 : :
71968 : :
72063 : :
72158 : :
72253 : :
72348 : :
72443 : :
72538 : :
72633 : :
72728 : :
72823 : :
72918 : :
73013 : :
73108 : :
73203 : :
73398 : :
73493 : :
73588 : :
73683 : :
73778 : :
73873 : :
73968 : :
74063 : :
74158 : :
74253 : :
74348 : :
74443 : :
74538 : :
74633 : :
74728 : :
74823 : :
74918 : :
75013 : :
75108 : :
75203 : :
75398 : :
75493 : :
75588 : :
75683 : :
75778 : :
75873 : :
75968 : :
76063 : :
76158 : :
76253 : :
76348 : :
76443 : :
76538 : :
76633 : :
76728 : :
76823 : :
76918 : :
77013 : :
77108 : :
77203 : :
77398 : :
77493 : :
77588 : :
77683 : :
77778 : :
77873 : :
77968 : :
78063 : :
78158 : :
78253 : :
78348 : :
78443 : :
78538 : :
78633 : :
78728 : :
78823 : :
78918 : :
79013 : :
79108 : :
79203 : :
79398 : :
79493 : :
79588 : :
79683 : :
79778 : :
79873 : :
79968 : :
80063 : :
80158 : :
80253 : :
80348 : :
80443 : :
80538 : :
80633 : :
80728 : :
80823 : :
80918 : :
81013 : :
81108 : :
81203 : :
81398 : :
81493 : :
81588 : :
81683 : :
81778 : :
81873 : :
81968 : :
82063 : :
82158 : :
82253 : :
82348 : :
82443 : :
82538 : :
82633 : :
82728 : :
82823 : :
82918 : :
83013 : :
83108 : :
83203 : :
83398 : :
83493 : :
83588 : :
83683 : :
83778 : :
83873 : :
83968 : :
84063 : :
84158 : :
84253 : :
84348 : :
84443 : :
84538 : :
84633 : :
84728 : :
84823 : :
84918 : :
85013 : :
85108 : :
85203 : :
85398 : :
85493 : :
85588 : :
85683 : :
85778 : :
85873 : :
85968 : :
86063 : :
86158 : :
86253 : :
86348 : :
86443 : :
86538 : :
86633 : :
86728 : :
86823 : :
86918 : :
87013 : :
87108 : :
87203 : :
87398 : :
87493 : :
87588 : :
87683 : :
87778 : :
87873 : :
87968 : :
88063 : :
88158 : :
88253 : :
88348 : :
88443 : :
88538 : :
88633 : :
88728 : :
88823 : :
88918 : :
89013 : :
89108 : :
89203 : :
89398 : :
89493 : :
89588 : :
89683 : :
89778 : :
89873 : :
89968 : :
90063 : :
90158 : :
90253 : :
90348 : :
90443 : :
90538 : :
90633 : :
90728 : :
90823 : :
90918 : :
91013 : :
91108 : :
91203 : :
91398 : :
91493 : :
91588 : :
91683 : :
91778 : :
91873 : :
91968 : :
92063 : :
92158 : :
92253 : :
92348 : :
92443 : :
92538 : :
92633 : :
92728 : :
92823 : :
92918 : :
93013 : :
93108 : :
93203 : :
93398 : :
93493 : :
93588 : :
93683 : :
93778 : :
93873 : :
93968 : :
94063 : :
94158 : :
94253 : :
94348 : :
94443 : :
94538 : :
94633 : :
94728 : :
94823 : :
94918 : :
95013 : :
95108 : :
95203 : :
95398 : :
95493 : :
95588 : :
95683 : :
95778 : :
95873 : :
95968 : :
96063 : :
96158 : :
96253 : :
96348 : :
96443 : :
96538 : :
96633 : :
96728 : :
96823 : :
96918 : :
97013 : :
97108 : :
97203 : :
97398 : :
97493 : :
97588 : :
97683 : :
97778 : :
97873 : :
97968 : :
98063 : :
98158 : :
98253 : :
98348 : :
98443 : :
98538 : :
98633 : :
98728 : :
98823 : :
98918 : :
99013 : :
99108 : :
99203 : :
99398 : :
99493 : :
99588 : :
99683 : :
99778 : :
99873 : :
99968 : :
100063 : :
100158 : :
100253 : :
100348 : :
100443 : :
100538 : :
100633 : :
100728 : :
100823 : :
100918 : :
101013 : :
101108 : :
101203 : :
101398 : :
101493 : :
101588 : :
101683 : :
101778 : :
101873 : :
101968 : :
102063 : :
102158 : :
102253 : :
102348 : :
102443 : :
102538 : :
102633 : :
102728 : :
102823 : :
102918 : :
103013 : :
103108 : :
103203 : :
103398 : :
103493 : :
103588 : :
103683 : :
103778 : :
103873 : :
103968 : :
104063 : :
104158 : :
104253 : :
104348 : :
104443 : :
104538 : :
104633 : :
104728 : :
104823 : :
104918 : :
105013 : :
105108 : :
105203 : :
105398 : :
105493 : :
105588 : :
105683 : :
105778 : :
105873 : :
105968 : :
106063 : :
106158 : :
106253 : :
106348 : :
106443 : :
106538 : :
106633 : :
106728 : :
106823 : :
106918 : :
107013 : :
107108 : :
107203 : :
107398 : :
107493 : :
107588 : :
107683 : :
107778 : :
107873 : :
107968 : :
108063 : :
108158 : :
108253 : :
108348 : :
108443 : :
108538 : :
108633 : :
108728 : :
108823 : :
108918 : :
109013 : :
109108 : :
109203 : :
109398 : :
109493 : :
109588 : :
109683 : :
109778 : :
109873 : :
109968 : :
110063 : :
110158 : :
110253 : :
110348 : :
110443 : :
110538 : :
110633 : :
110728 : :
110823 : :
110918 : :
111013 : :
111108 : :
111203 : :
111398 : :
111493 : :
111588 : :
111683 : :
111778 : :
111873 : :
111968 : :
112063 : :
112158 : :
112253 : :
112348 : :
112443 : :
112538 : :
112633 : :
112728 : :
112823 : :
112918 : :
113013 : :
113108 : :
113203 : :
113398 : :
113493 : :
113588 : :
113683 : :
113778 : :
113873 : :
113968 : :
114063 : :
114158 : :
114253 : :
114348 : :
114443 : :
114538 : :
114633 : :
114728 : :
114823 : :
114918 : :
115013 : :
115108 : :
115203 : :<

1) File Name: Lost Highway 1997 720p BRRip x264 RmD (HDScene Release).mkv
 Last Accessed: 09/25/12 09:40:19PM
 File Created: 09/21/12 11:54:21PM
 File Full Path: JRaleigh\MacBook C02HW056DV31\D\Macintosh HD\Users\jr\Desktop\Movies\Lost Highway 1997 720p BRRip x264 RmD (HDScene Release)\Lost Highway 1997 720p BRRip x264 RmD (HDScene Release).mkv

2) File Name: no country for old men [vose] dvdrip xvid mp3.avi
 Last Accessed: 11/04/13 09:43:05AM
 File Created: 01/03/12 09:53:01PM
 Full Path: JRaleigh\MacBook C02HW056DV31\D\Macintosh HD\Users\jr\Desktop\Movies\no country for old men [vose] dvdrip xvid mp3.avi

Using EnCase software a keyword search for “torrent” was conducted. Upon examining the search hits I located a text file named “David_Cesolini_Chats.txt” that contained a discussion about torrents. Further examination revealed that this chat and other files contained in a folder “Chinga_La_Migra_Dos” may be related to a hacking event that took place in 2011. This computer contains the sensitive files released by hacker(s) which contain individuals’ personal information including social security, driver’s license numbers, account passwords etc.

```
177880 David: yeah - whassup?
177904 9:35 PM me: just checked my torrent
177940 1. SMB
177948 download speed
177965 hahahahaha
177980 David: i think i have a crappy torrent
178020 i'm at 1.2kb
178035 me: lol
178044 i also have 120 seeders
178070 David: you and your seeders
178099 9:36 PM me: dork
178116 this is now a new movie
178142 The Book of Eli
178160 David: i should try to get toy story 3
178200 me: its not out yet
178221 I only want things with excellent quality and excellent sound. cause i watch them through my PS3
178320 9:37 PM David: i'm downloading toy story 3 now - it's going much faster. i'll let you know if it's good
178424 9:38 PM me: you go through isohunt?
178456 me: do you keep all your downloads after use or delete
178512 David: delete
178527 me: i do a google search for a torrent
178567 either piratebay or kickassTorrent
178603 David: cool
178616 me: isohunt sometimes
178639 David: gotta be careful for viruses
178676 9:39 PM kickass usually has the better stuff
178732 i delete everything in the torrent besides the movie. then transfer to ps3, I dont open it on my pc at all.
178842 so most virus if any are formatted for pc's
178887 9:40 PM David: gotcha. although if you get a ps3 virus, you're screwed. how do you clean a ps3?
178958 me: just format. so I loose my saved data boohoo
179035 9:41 PM and if it breaks its under warranty
179079 9:42 PM David: when am i getting froyo?
179119 me: i want to find a new version of Chrome OS. But nothing you would think something would've gotten leaked by now.
179236 Thats a good question
179260 hahaha
```

JRaleigh\MacBook C02HW056DV31\D\Macintosh HD\Users\jr\Scrap Pile\Old Swap Drive\Chinga_La_Migra_Dos\David_Cesolini_Chats.txt (PS 820063431 LS 819653791 CL 102456723 SO 236 PO 179948 LE 1)

EnCase screen capture of sensitive data relating to “Chinga_La_Migra_Dos” redacted:

The screenshot shows the EnCase Forensic interface. On the left, there is a file tree view of the disk structure. A specific folder, "Chinga_La_Migra_Dos", is expanded, showing various subfolders like "DataTables-1.7.6", "Driver", "English", and "essentialdesignpatterns1". To the right of the file tree is a detailed list of files with their names, file types (txt), and timestamps. The list includes files such as Donald_Nathaniel.txt, David_J_Basadua.txt, Edward_Connelly.txt, David_Cesolini_Chats.txt, David_Cesolini.txt, Gene_Moran.txt, Joseph_Wilson.txt, Christopher_Sabo.txt, Richard_Wooten.txt, Robert_J_Barry.txt, and Briare_Campbell.txt. The timestamps range from 06/24/12 04:21:34PM to 06/29/11 10:31:54AM. Below the file tree and list, there is a large text area containing numerous sensitive data entries, many of which are redacted with black bars. These entries include email addresses, phone numbers, and other personal information. At the bottom of the text area, there is a URL: http://dot3media.com/wp-login.php, a user name: royley, and a password: v... . There are also entries for DIRECTV.com, a phone number (928) 916-8177, and a Voicemail Retrieval number (714) ... 214.

Located Torrent Files

- 1) File Name: test.torrent
 Last Accessed: 09/04/14 02:43:50PM
 File Created: 03/18/14 02:49:46PM
 Full Path: JRaleigh\MacBook C02HW056DV31\D\Macintosh HD\Applications\Development\LightTable\LightTable.app\Contents\Resources\app.nw\core\node_modules\bencode\benc hmark\test.torrent
- 2) File Name: xubuntu-13.04-desktop-i386.iso.torrent
 Last Accessed: 09/15/14 08:57:29AM
 File Created: 04/25/13 06:28:19AM
 Full Path: JRaleigh\MacBook C02HW056DV31\D\Macintosh HD\Users\jr\Downloads\xubuntu-13.04-desktop-i386.iso.torrent

Windows XP Parallels Virtual Machine Located in the following location:

1. JRaleigh\MacBook C02HW056DV31\D\Macintosh HD\Users\jr\Documents\Parallels\Windows 7.pvm\Windows 7-0.hdd\Windows 7-0.hdd.0.{5fbaabe3-6958-40ff-92a7-860e329aab41}.hds
 2. JRaleigh\MacBook C02HW056DV31\D\Macintosh HD\Users\jr\Documents\Parallels\Windows XP Old.pvm\Windows XP.hdd\Windows XP.hdd.0.{5fbaabe3-6958-40ff-92a7-860e329aab41}.hds

Parallels Desktop software is hardware virtualization software for the MAC operating system. Parallels software allows the user to create and run virtual operating systems including Windows based operating systems on a MAC computer. In this case the user was utilizing a Microsoft Windows XP virtual machine with Parallels Software. Using EnCase software I copied out the virtual machine “Windows XP.hdd.0.{5fbaabe3-6958-40ff-92a7-860e329aab41}.hds” along with the companion configuration files to my local forensics machine. Using software “VMware vCenter Converter Standalone Client” I converted the image to a VMware virtual machine and loaded the image into IEF forensic software for processing. The same process was followed for the Windows 7 Parallels virtual machine however the configurations appeared to be corrupt.

Operating System Information

Operating System	Microsoft Windows XP
Operating System Version	-Not Found-
Build Number	2600
Version Number	5.1
Product ID	76487-OEM-0054883-52515
Product Key	DQGQ7-R6MVP-KPBKY-PWVY88-47FYJ
Last Service Pack	Service Pack 3
Owner	Jesse Raleigh
Organization	(not found)
Install Date/Time - (UTC-7:00) (MM/dd/yyyy)	07/22/2010 10:44:09 AM
Last Shutdown Date/Time - (UTC-7:00) (MM/dd/yyyy)	01/23/2014 10:38:58 AM
System Root	C:\WINDOWS
Path	C:\WINDOWS
Source	Raleigh.vmdk - Partition 1 (Microsoft NTFS, 7 GB) (All Files and Folders) - [ROOT]\WINDOWS\system32\config\software
Located At	Registry Key: MicrosoftWindows NT\CurrentVersion, ControlSet001\Control\Windows
Evidence Number	Raleigh

User Account Information

User Name	Type of User	Security Identifier	User Group(s)	Last Login Date/Time - (UTC-7:00) (MM/dd/yyyy)	Last Password Change Date/Time - (UTC-7:00) (MM/dd/yyyy)	Login Count	Account Disabled	Password Required
Administrator	Local User	500	Administrators		07/22/2010 06:31:25 AM	0	False	True
Guest	Local User	501	Guests			0	True	False
HelpAssistant	Local User	1000			07/22/2010 10:35:04 AM	0	True	True
SUPPORT_3889	Local User	1002	HelpServicesGroup		07/22/2010 10:38:42 AM	0	True	True
Jesse	Local User	S-1-5-21-789336058-	Administrators	01/23/2014 10:38:12 AM	07/22/2010 10:56:37 AM	371	False	True
ASPNET	Local User	1004	Users		10/21/2013 08:25:55 AM	0	False	False

Windows XP Parallels Virtual Machine Findings

Using IEF (Internet Evidence Finder) and EnCase software I searched and identified all the videos on the drive and could not locate any responsive data. I located uTorrent client software on the machine and LNK file in the start menu of computer user Jesse.

Linked Path	C:\Documents and Settings\Jesse\Application Data\Parallels\Shared Applications\utorrent (Mac).exe
Arguments	(not found)
Created Date/Time - (UTC-7:00) (MM/dd/yyyy)	01/03/2011 02:58:02 PM
Last Modified Date/Time - (UTC-7:00) (MM/dd/yyyy)	01/03/2011 02:58:02 PM
Last Accessed Date/Time - (UTC-7:00) (MM/dd/yyyy)	04/18/2013 11:19:21 AM
Target File Created Date/Time - (UTC-7:00) (MM/dd/yyyy)	01/03/2011 02:58:02 PM
Target File Last Modified Date/Time - (UTC-7:00) (MM/dd/yyyy)	01/03/2011 02:58:02 PM
Target File Last Accessed Date/Time - (UTC-7:00) (MM/dd/yyyy)	01/03/2011 02:58:02 PM
Target Attributes	FILE_ATTRIBUTE_ARCHIVE
Drive Type	DRIVE_FIXED
Serial Number	F4A72673
Volume Name	(not found)
Show Command	SW_SHOWNORMAL
Net Bios Name	jesse-b3e74a8a
Mac Address	0:1C:42:4E:E2:20
Target File Size (Bytes)	228864
Source	Raleigh.vmdk - Partition 1 (Microsoft NTFS, 7 GB) (All Files and Folders) - [ROOT]\Documents and Settings\Jesse\Start Menu\Programs\Parallels Shared Applications\utorrent (Mac).lnk

Using EnCase and IEF software I searched for possible network storage locations. NetHood which corresponds to %USERPROFILE%\NetHood, contains only LAN shared folder path (server and folder name). NetHood stores the path to the folder containing shortcuts to servers that the user has added to My Network Places. This indicates additional file storage somewhere on the local network. IEF located locations on the network including “PSF” where folders are being accessed including “\\psf\Parallels Desktop” 7&8. The Parallels Desktop folder 7&8 indicate possible existence of other virtual machines or where various versions of Parallels software resides. I exported IEF’s complete list of Network Share Information and Shellbags to the final report case files folder under “MacBook C02HW056DV31_JRaleigh_LT1\Windows XP Parallels Virtual Machine Files”.

	Name	Physical Size	File Ext	Full Path	Is Deleted	Last Accessed	File Created
<input type="checkbox"/> 1	file c on 10.10.10.42	256	42	RaleighVM\Raleigh\C\Documents and Settings\Jesse\NetHood\c on 10.10.10.42	No	07/29/13 05:07:09PM	06/05/12 10:21:24PM
<input type="checkbox"/> 2	file c on 10.10.10.7	256	7	RaleighVM\Raleigh\C\Documents and Settings\Jesse\NetHood\c on 10.10.10.7	No	07/29/13 05:07:09PM	08/13/12 08:31:43AM
<input type="checkbox"/> 3	file c on Ch4 (10.10.10.39)	256	39	RaleighVM\Raleigh\C\Documents and Settings\Jesse\NetHood\c on Ch4 (10.10.10.39)	No	07/29/13 05:07:09PM	06/05/12 06:40:34PM
<input type="checkbox"/> 4	file c on Phillips (10.10.10.6)	256	6)	RaleighVM\Raleigh\C\Documents and Settings\Jesse\NetHood\c on Phillips (10.10.10.6)	No	07/29/13 05:07:09PM	10/01/12 10:34:30AM
<input type="checkbox"/> 5	file c on Swan (10.10.10.46)	256	46)	RaleighVM\Raleigh\C\Documents and Settings\Jesse\NetHood\c on Swan (10.10.10.46)	No	07/29/13 05:07:09PM	06/05/12 10:25:42PM
<input type="checkbox"/> 6	file Home on psf	256		RaleighVM\Raleigh\C\Documents and Settings\Jesse\NetHood\Home on psf	No	07/29/13 05:07:09PM	06/05/12 06:39:06PM
<input type="checkbox"/> 7	filexampp on 10.10.10.8	256	8	RaleighVM\Raleigh\C\Documents and Settings\Jesse\NetHood\xampp on 10.10.10.8	No	07/29/13 05:07:09PM	05/22/12 05:01:32PM
<input type="checkbox"/> 8	file c on 10.10.10.26	256	26	RaleighVM\Raleigh\C\Documents and Settings\Jesse\NetHood\c on 10.10.10.26	No	12/16/13 10:01:23PM	05/23/12 01:45:17PM

IEF screen capture of Network Share Information for "\psf\"

The screenshot shows the IEF Report Viewer interface with the title "IEF Report Viewer v6.5.1.0668 - Case: JRaleigh". The left sidebar displays a tree view of recovered artifacts, including "Recovered Artifacts" (43 items) and "Operating System" (50 items). The main pane shows a table of network shares with columns: #, Network Name, Connection Type, Account, Last Modified D., and Mapped_. The table lists 36 entries, with row 34 ("\\psf\\Parallels Desktop 7") highlighted in yellow. Below the table is a search bar and a message indicating "Showing results 1 - 50 of 50". A detailed view of the selected entry (row 34) is shown in a modal window, listing fields such as Network Name, Mapped Drive Letter, Connection Type, Provider Name, Account, Last Modified Date/Time, Source, Located At, and Evidence Number.

#	Network Name	Connection Type	Account	Last Modified D.	Mapped_
25	\psf\JR Backup	Drive Redirection	Jesse	12/17/2013 07:38...	
26	\psf\Messages Beta	Drive Redirection	Jesse	06/05/2012 04:37...	
27	\psf\Microsoft Office 2011 14.2.3 Update	Drive Redirection	Jesse	02/19/2013 06:40...	
28	\psf\Microsoft Office 2011 14.3.5 Update	Drive Redirection	Jesse	07/01/2013 01:58...	
29	\psf\MobileBackups	Drive Redirection	Jesse	12/16/2013 08:01...	
30	\psf\MySQL Workbench	Drive Redirection	Jesse	04/18/2013 11:19...	
31	\psf\NeatWorksForMac	Drive Redirection	Jesse	05/23/2012 09:08...	
32	\psf\NO NAME	Drive Redirection	Jesse	05/02/2013 08:59...	
33	\psf\Opera Mobile Emulator	Drive Redirection	Jesse	07/30/2013 08:47...	
34	\psf\Parallels Desktop 7	Drive Redirection	Jesse	01/23/2012 09:24...	
35	\psf\Parallels Desktop 8	Drive Redirection	Jesse	03/21/2013 09:12...	
36	\psf\PosiTector	Drive Redirection	Jesse	07/30/2013 10:41...	

JRaleigh_RT2" aka "MacBook 340269NBATMTime Zone Settings

JRaleigh\MacBook 340269NBATM\1 Macintosh HD\Macintosh HD\private\etc\localtime
Configured Time Zone:America/Detroit

/usr/share/zoneinfo/America/Detroit

OS Information

ProductBuildVersion: 13F34
ProductCopyright: 1983-2014 Apple Inc.
ProductName: Mac OS X
ProductUserVisibleVersion: 10.9.5
ProductVersion: 10.9.5

User Information

	Name	File Ext	Last Accessed	File Created	Full Path
1	.localized	localized	08/25/13 04:58:39AM	08/25/13 04:58:39AM	JRaleigh\MacBook 340269NBATM\1 Macintosh HD\Macintosh HD\Users\localized
2	heather		06/24/12 05:38:39PM	06/24/12 10:29:51AM	JRaleigh\MacBook 340269NBATM\1 Macintosh HD\Macintosh HD\Users\heather
3	j		07/27/11 01:44:50PM	07/27/11 01:44:50PM	JRaleigh\MacBook 340269NBATM\1 Macintosh HD\Macintosh HD\Users\j
4	jr		06/24/12 05:39:09PM	07/27/10 12:51:33AM	JRaleigh\MacBook 340269NBATM\1 Macintosh HD\Macintosh HD\Users\jr
5	Ove		04/17/13 11:15:35PM	04/17/13 11:15:26PM	JRaleigh\MacBook 340269NBATM\1 Macintosh HD\Macintosh HD\Users\Ove
6	Shared		02/17/14 08:26:14AM	06/13/11 12:52:36PM	JRaleigh\MacBook 340269NBATM\1 Macintosh HD\Macintosh HD\Users\Shared

JRaleigh_RT2" aka "MacBook 340269NBATM Findings:

A search of the hard drive for evidence relating to Malibu Media movies was negative. A search of the hard drive evidence of BitTorrent use was positive.

1. Located several BitTorrent related website URLs pertaining to the website "The Pirate Bay". Please refer to the Final Report Case Files folder for this device "Pirate Bay URLs".

UTorrent installed on Computer

Name uTorrent
 Is Deleted No
 Last Accessed 12/03/14 02:16:47PM
 File Created 01/30/12 09:30:08AM
 Last Written 01/30/12 09:30:08AM
 File Acquired 12/03/14 04:02:13PM
 Physical Location 388,321,886,208
 Physical Sector 758,441,184
 Evidence File MacBook 340269NBATM
 Full Path JRaleigh\MacBook 340269NBATM\1 Macintosh HD\Macintosh HD\Applications\uTorrent.app\Contents\MacOS\uTorrent

Numerous Music MP3 files have embedded metadata referencing "www.torrentazos.com" indicating their possible origin. The website "www.torrentazos.com" is a website where user can illegally obtain music, movies etc.

	Name	Preview	Hit Text
74	05 The Rape Over.mp3	ON East Coast RapUFID http://musicbrainz.org COMM c0 www.torrentazos.comTRCK 5/18TPOS DAPIC w image/png %PNG IHDR .torrent	
75	06 - I Got Bass.mp3	k On My Shit!TRCK 6TYER 2009TCOM Hip-HopCOMM eng www.torrentazos.comTLAN EnglishCOMM h engiTunNORM 00000BD1 00000B54 00003A .torrent	
76	06 - I Got Bass.mp3	k On My Shit!TRCK 6TYER 2009TCOM Hip-HopCOMM eng www.torrentazos.comTLAN EnglishCOMM h engiTunNORM 00000BD1 00000B54 00003A .torrent	
77	06 - Walk This Way.mp3	Aerosmith Devil's Got A New Disguise (Th2006www.torrentazos.com	
78	06 - Walk This Way.mp3	Walk This WayTRCK 6TYER 2006TCOM RockCOMM eng www.torrentazos.comTALB 8 Devil's Got A New Disguise (The Very Best Of Aerosmith)TP .torrent	
79	06 Drive Slow (ft. Paul Wall & Glc).mp3	ate RegistrationTYER 2005TRCK 6TCOM (15)COMM spa www.torrentazos.comTPE1 Kanye WestCOMM h engiTunNORM 0000080E 00000B58 0000 .torrent	
80	06 Hate that I Love You (Feat. Ne-Yo).mp3	ood Girl Gone BadTRCK 6TYER 2007TCOM R&BCOMM eng www.torrentazos.comTLAN EnglishCOMM h engiTunNORM 00000A85 00000B2C 00003F .torrent	
81	06 Metal Heart.mp3	Bleed Like MeTRCK 6TYER 2005TCOM RockCOMM \$ eng www.torrentazos.com By FEFE2003APIC dD image/png %PNG IHDR ô ô B% È .torrent	
82	06 Nothing's The Same.mp3	006TCOM Hard RockUFID http://musicbrainz.org COMM c0 www.torrentazos.comTXXX MusicBrainz Artist Id TXXX musicbrainz_artistid TRC .torrent	
83	06 Silver.mp3	Rain TRCK 6 TYER 2007 TCOM Heavy Metal COMM eng www.torrentazos.com .torrent	
84	07 - Dude (Looks Like A Lady).mp3	dy) Aerosmith Devil's Got A New Disguise (Th2006www.torrentazos.com .torrent	
85	07 - Dude (Looks Like A Lady).mp3	ols Like A Lady)TRCK 7TYER 2006TCOM RockCOMM eng www.torrentazos.comTALB 8 Devil's Got A New Disguise (The Very Best Of Aerosmith)TP .torrent	
86	07 - Girls Love Me feat. Rick Ross.mp3	k On My Shit!TRCK 7TYER 2009TCOM Hip-HopCOMM eng www.torrentazos.comTLAN EnglishCOMM h engiTunNORM 00000FCF 00001150 00007F .torrent	
87	07 Bedstuy Parade & Funeral March.mp3	ON East Coast RapUFID http://musicbrainz.org COMM c0 www.torrentazos.comTRCK 7/18TPOS DAPIC w image/png %PNG IHDR .torrent	
88	07 Civilize The Universe.mp3	Rain TRCK 7 TYER 2007 TCOM Heavy Metal COMM eng www.torrentazos.com .torrent	
89	07 Hell Is High.mp3	hot To HellTRCK 7TYER 2006TCOM Hard RockCOMM eng www.torrentazos.comTLAN engCOMM h engiTunNORM 00002359 00002EDE 00000910D .torrent	
90	07 My Way Home (ft. Common).mp3	ate RegistrationTYER 2005TRCK 7TCOM (15)COMM spa www.torrentazos.comTPE1 Kanye WestCOMM h engiTunNORM 000004D8 000004D9 000 .torrent	
91	07 Say It.mp3	ood Girl Gone BadTRCK 7TYER 2007TCOM R&BCOMM eng www.torrentazos.comTLAN EnglishCOMM h engiTunNORM 00000972 00000942 000065 .torrent	
92	07 Sex Is Not The Enemy.mp3	Bleed Like MeTRCK 7TYER 2005TCOM RockCOMM \$ eng www.torrentazos.com By FEFE2003APIC dD image/png %PNG IHDR ô ô B% È .torrent	
93	07 What Else Is There.mp3	05TCOM ElectronicUFID http://musicbrainz.org COMM " c0 www.torrentazos.com By FEFETRCK 7TPOS OTLAN EnglishCOMM h engiTun .torrent	
94	08 - Blown feat. T-Pain.mp3	k On My Shit!TRCK 8TYER 2009TCOM Hip-HopCOMM eng www.torrentazos.comTLAN EnglishCOMM h engiTunNORM 00000B04 00000B30 00004A .torrent	
95	08 - Rag Doll.mp3	Aerosmith Devil's Got A New Disguise (Th2006www.torrentazos.com .torrent	
96	08 - Rag Doll.mp3	2 Rag DollTRCK 8TYER 2006TCOM RockCOMM eng www.torrentazos.comTALB 8 Devil's Got A New Disguise (The Very Best Of Aerosmith)TP .torrent	

Located Torrent Files

1) File Name: cablegate-201011290900.7z.torrent

Last Accessed: 06/22/12 02:02:02PM

File Created: 11/29/10 08:18:17AM

Full Path: JRaleigh\MacBook 340269NBATM\1 Macintosh HD\Macintosh HD\Users\jr\Library\Application Support\uTorrent\cablegate-201011290900.7z.torrent

2) File Name: Chinga La Migra.torrent

Last Accessed: 06/22/12 02:02:02PM

File Created: 06/24/11 09:39:07AM

Full Path: JRaleigh\MacBook 340269NBATM\1 Macintosh HD\Macintosh HD\Users\jr\Library\Application Support\uTorrent\Chinga La Migra.torrent

3) File Name: Chinga_La_Migra_Dos.torrent

Last Accessed: 06/22/12 02:02:02PM

File Created: 06/29/11 10:27:31AM

Full Path: JRaleigh\MacBook 340269NBATM\1 Macintosh HD\Macintosh HD\Users\jr\Library\Application Support\uTorrent\Chinga_La_Migra_Dos.torrent

4) File Name: MMM_Booz_Allen.torrent

Last Accessed: 06/22/12 02:02:02PM

File Created: 07/11/11 02:34:41PM

Full Path: JRaleigh\MacBook 340269NBATM\1 Macintosh HD\Macintosh HD\Users\jr\Library\Application Support\uTorrent\MMM_Booz_Allen.torrent

5) File Name: NeoOffice-3.1.2-Intel.dmg.torrent

Last Accessed: 06/22/12 02:02:02PM

File Created: 02/11/11 11:37:50PM

Full Path: JRaleigh\MacBook 340269NBATM\1 Macintosh HD\Macintosh HD\Users\jr\Library\Application Support\uTorrent\NeoOffice-3.1.2-Intel.dmg.torrent

6) File Name: Zenith.Part.1.2011.720p.x264-VODO.torrent

Last Accessed: 06/22/12 02:02:02PM

File Created: 03/20/11 09:09:03AM

Full Path: JRaleigh\MacBook 340269NBATM\1 Macintosh HD\Macintosh HD\Users\jr\Library\Application Support\uTorrent\Zenith.Part.1.2011.720p.x264-VODO.torrent

7) File Name: sDgo3FDksdGwsrkrS.enc.torrent

Last Accessed: 06/22/12 02:02:02PM

File Created: 08/31/11 02:30:15PM

Full Path: JRaleigh\MacBook 340269NBATM\1 Macintosh HD\Macintosh HD\Users\jr\Library\Application Support\uTorrent\sDgo3FDksdGwsrkrS.enc.torrent

8) File Name: cablegate-201108300212.7z.torrent

Last Accessed: 06/22/12 02:02:02PM

File Created: 09/02/11 12:07:41AM

Full Path: JRaleigh\MacBook 340269NBATM\1 Macintosh HD\Macintosh HD\Users\jr\Library\Application Support\uTorrent\cablegate-201108300212.7z.torrent

9) File Name: 404EC54D29D940D04485756D7500745F8CFF10C3.torrent

Last Accessed: 06/22/12 02:02:02PM

File Created: 02/07/12 12:02:12AM

Full Path: JRaleigh\MacBook 340269NBATM\1 Macintosh HD\Macintosh HD\Users\jr\Library\Application Support\uTorrent\404EC54D29D940D04485756D7500745F8CFF10C3.torrent

10) File Name: American Survival Guide Magazine.torrent

Last Accessed: 06/22/12 02:02:02PM

File Created: 03/03/12 12:17:16PM

Full Path: JRaleigh\MacBook 340269NBATM\1 Macintosh HD\Macintosh HD\Users\jr\Library\Application Support\uTorrent\American Survival Guide Magazine.torrent

11) File Name: BT5R2-GNOME-32.torrent

Last Accessed: 06/22/12 02:02:02PM

File Created: 05/05/12 11:07:56PM

Full Path: JRaleigh\MacBook 340269NBATM\1 Macintosh HD\Macintosh HD\Users\jr\Library\Application Support\uTorrent\BT5R2-GNOME-32.torrent

12) File Name: THE METEORS - [WWW.PunksAndSkins.COM] - 13 ALBUMS.torrent

Last Accessed: 06/22/12 02:02:02PM

File Created: 06/06/12 11:02:29PM

Full Path: JRaleigh\MacBook 340269NBATM\1 Macintosh HD\Macintosh HD\Users\jr\Library\Application Support\uTorrent\THE METEORS - [WWW.PunksAndSkins.COM] - 13 ALBUMS.torrent

13) File Name: Demented Are Go.torrent

Last Accessed: 06/22/12 02:02:02PM

File Created: 06/06/12 11:19:35PM

Full Path: JRaleigh\MacBook 340269NBATM\1 Macintosh HD\Macintosh HD\Users\jr\Library\Application Support\uTorrent\Demented Are Go.torrent

Located USB Device Connection Information

Using EnCase software I conducted a keyword search of the “system.log” files located on both laptop computers using the keyword “USBMSC”. Using the keyword “USBMSC” I was able to locate and identify USB devices that were plugged into the laptop computers. The following is a bookmark list of the keyword search hits.

1) File Name: system.log.0 (Zip File Volume)

Last Accessed: 12/03/14 01:25:13AM

File Created: 12/03/14 01:25:13AM

Comments: Identified as a Western Digital Technologies, Inc. My Book Essential (WDBACW) (External USB Hard Drive 1-3TB in size depending on the exact model) Keyword searching indicates a model “1140” which is a 2TB hard drive.

Full Path: JRaleigh\MacBook C02HW056DV31\Device\private\var\log\system.log.0.gz\GZIP Volume\system.log.0

Dec 2 08:27:16 jrmfp kernel[0]: USBMSC Identifier (non-unique): 574D415A4139303734343136 0x1058 0x1140 0x1012,

In order to decode the values associated with these entries you need to look at the source code for IOUSBInterface.cpp from opensource.apple.com. Using the above note data you can see that the three values: 0x1058 0x1140 0x1012 are the Vendor ID, Product ID and the Device Release number:

```
// these properties come from the device descriptor, but can be used for interface matching
setProperty(kUSBVendorID, (unsigned long long)_device->GetVendorID(), (sizeof(UInt16) * 8));
setProperty(kUSBProductID, (unsigned long long)_device->GetProductID(), (sizeof(UInt16) * 8));
setProperty(kUSBDeviceReleaseNumber, (unsigned long long)_device->GetDeviceRelease(), (sizeof(UInt16) * 8));
```

In this case looking online at the most up to date database: <http://www.linux-usb.org/usb.ids> one can see that 0x1058 (1058) is from Western Digital Technologies, Inc. and 0x1140 (1140) is a My Book Essential (WDBACW) and 0x1012 (1012) is the release for that drive.

Using EnCase software I conducted a keyword search for serial number “574D415A4139303734343136” pertaining to the Western Digital My Book Essentials External USB hard drive. I located evidence that this device was plugged into both laptop computers numerous times. The search hits were exported out and are viewable by reviewing the final report case files folder named “USB Device Search Hits”.

1. **JRaleigh_LT1” aka “MacBook C02HW056DV31** – Numerous search hits in the Parallels.log file, unallocated space and “2014.12.02.U0.G80.asl” indicate evidence of connection from 7/10/2013 to 12/2/2014.
2. **JRaleigh_RT2” aka “MacBook 340269NBATM** – Numerous search hits in the Parallels.log file, unallocated space and “dispatcher.desktop.xml” indicate evidence of connection from 10/13/2011 to 2/17/2014.

EnCase Screen Captures of the system.log file JRaleigh_LT1” aka “MacBook C02HW056DV31 from 12/2/2014

```

051318Dec 2 08:26:44 ryLimit key is not available on this platform.
051365Dec 2 08:26:44 --- last message repeated 1 time ---
051418Dec 2 08:26:44 jrbmp locationd[227]: Location icon should now be in state 'Inactive'
051504Dec 2 08:26:45 jrbmp com.apple.SecurityServer[65]: Session 100077 created
051579Dec 2 08:26:45 jrbmp login[79]: -[SessionManager getClient:withRole:inAuditSession:]::241: ERROR: No session dictionary
051699 for audit session 100077
051725Dec 2 08:26:45 jrbmp login[79]: _SMGetSessionAgent:73: ERROR: _SMGetClientForAuditSessionAgent failed 2
051832Dec 2 08:26:45 jrbmp IMRemoteURLConnectionAgent[14771]: SACHShieldWindowShowing:925: ERROR: NULL response
051938Dec 2 08:26:45 jrbmp soagent[492]: Can't allocate SOHelper <SOMessageHelper: 0x7fc32065b930> inside com.apple.soagent
052057Dec 2 08:27:03 jrbmp sandbox[302] ((14703)): netbiosd(14703) deny mach-lookup com.apple.networkd
052156Dec 2 08:27:08 jrbmp thermald[31]: invalid attribute or value, default to yes
052235Dec 2 08:27:08 jrbmp clouddd[297]: Stream 0x7fbfd132614c0 is sending an event before being opened
052332Dec 2 08:27:12 jrbmp iTunes[6288]: Entered:_AMMuxedDeviceDisconnected, Device Serial # 0x1058
052418Dec 2 08:27:12 jrbmp iTunes[6288]: Entered:_thr_AMMuxedDeviceDisconne
052509Dec 2 08:27:12 jrbmp iTunes[6288]: tid:9a73 - Mux ID not found in mapping dictionary
052595Dec 2 08:27:12 jrbmp iTunes[6288]: tid:9a73 - Can't handle disconnect with invalid acid
052684Dec 2 08:27:12 jrbmp thermald[31]: invalid attribute or value, default to yes
052763Dec 2 08:27:13 --- last message repeated 1 time ---
052816Dec 2 08:27:13 jrbmp sandbox[302] ((14741)): icbaccounts(14741) deny mach-lookup com.apple.CrashReporterSupportHelper
052936
052937Dec 2 08:27:16 jrbmp kernel[0]: USBMSC Identifier (non-unique): 574D415A4139303734343136 0x1058 0x1140 0x1012, 3
053051Dec 2 08:27:16 jrbmp iTunes[6288]: Entered:_AMMuxedVersion2DeviceConnected, mux-device:66
053142Dec 2 08:27:16 jrbmp iTunes[6288]: tid:278b3 - unable to query device capabilities
053226Dec 2 08:27:25 jrbmp AppleMobileBackup[14787]: WARNING: Backing up 8e8ae696fa4c736c20d09c109b421c88elf78f1a
053335Dec 2 08:27:33 jrbmp nsurlsession[228]: Being asked if container with identifier com.apple.clouddocs.F3LWYJ7GM7.com.ap
053455ple.garageband10 is foreground before getting callback from BRContainersMonitor!
053536Dec 2 08:27:37 --- last message repeated 1 time ---
053589Dec 2 08:27:37 jrbmp nsurlsession[228]: Being asked if container with identifier com.apple.clouddocs.VUY5YR82Y5.com.bi
053709naryhammer.3030 is foreground before getting callback from BRContainersMonitor!
053789Dec 2 08:27:39 --- last message repeated 1 time ---
053842Dec 2 08:27:39 jrbmp kernel[0]: CoreStorage: fsck_cs has finished for group "418553EF-3979-415D-BB19-47B896EAC392" with
053962 status 0x00
053975Dec 2 08:27:39 jrbmp com.apple.kextd[28]: LVG changed
054030Dec 2 08:27:39 jrbmp kernel[0]: CoreStorageFamily::unlockVEKs(9209BAB1-7DE0-4DD7-994F-C17E40377668) VEK unwrap failed.
054150this is normal, except for the root volume.
054194Dec 2 08:27:39 jrbmp com.apple.kextd[28]: LVG changed

```

JRaleigh|MacBook C02HW056DV31|D|Macintosh HD|private|var|log|system.log.0.gz|GZIP Volume|system.log.0 (system.log.0.gz: P50 LS0 CL0 SO010 FO51724 LE1)

EnCase Screen Captures of the system.log file JRaleigh_LT1” aka “MacBook C02HW056DV31 from 12/1/2014

```

015369235446Dec 1 11:56:22 jrbmp com.apple.AmbientDisplayAgent[6214]: AMBD initializing devices
015369235531Dec 1 11:56:22 jrbmp WindowServer[147]: CGXSetDisplayColorProfileAndTransfer: Display 0x0424lead: Unit 1; ColorProfile
015369235651{ -790678564 }; TransferTable (256, 12)
015369235691Dec 1 11:56:22 jrbmp com.apple.AmbientDisplayAgent[6214]: AMBD Agent: xpc connection became invalid during event handle
015369235811r
015369235813Dec 1 11:56:26 jrbmp kernel[0]: USBMSC Identifier (non-unique): 574D415A4139303734343136 0x1058 0x1140 0x1012, 3
015369235927Dec 1 11:56:27 jrbmp kernel[0]: AppleUSBEthernetHost::powerStateChangeOccurred: intf is not enabled, ignoring ... st:
0153692360470
015369236049Dec 1 11:56:27 jrbmp kernel[0]: en4: attached with 4 suspended link-layer multicast membership(s)
015369236148Dec 1 11:56:27 jrbmp kernel[0]: AppleUSBEthernetHost::enable: Interface already enabled
015369236237Dec 1 11:56:27 jrbmp kernel[0]: en4: successfully restored 4 suspended link-layer multicast membership(s) (err=0)
015369236352Dec 1 11:56:27 jrbmp iTunes[6288]: Entered:_AMMuxedVersion2DeviceConnected, mux-device:49

```

JRaleigh|MacBook C02HW056DV31|D|Unallocated Clusters (PS 688213750 LS 687804110 CL 85975513 SO 390 FO 15369235846 LE6)

EnCase Screen Captures of a Parallels.log file in unallocated space JRaleigh_LT1" aka "MacBook C02HW056DV31 from 12/16/2013

```
00815013568712-16 12:57:52.505 F /gui:343:707/ localhost: received result for [DspCmdUserGetHostHwInfo]. RC = [PRL_ERR_SUCCESS]
00815013580312-16 12:57:57.315 F /disp:656:8303/ On enter : dev_type = 15 dev_name = 15100000 event_code = 1
00815013590212-16 12:57:57.541 F /disp:656:8303/ USB connected (autoconnect) <15100000|1058|1140|super|--|574D415A4139303734343136>
008150136022<My Book 1140> <PUDT_DISK_STORAGE>
00815013605712-16 12:57:57.542 F /disp:656:8303/ USB GUI notify '' <15100000|1058|1140|super|--|574D415A4139303734343136> <My Book 1
008150136177140> <PUDT_DISK_STORAGE>
00815013620212-16 12:57:57.544 F /disp:656:8303/ make post to autoconnect event from thread notifier! strDevImage == 15100000|1058|1
008150136322140|super|--|574D415A4139303734343136 uiDevState==1
00815013637412-16 12:57:57.546 F /disp:656:8303/ USB VM notify 'connect' <15100000|1058|1140|super|--|574D415A4139303734343136> <My
008150136494Book 1140> <PUDT_DISK_STORAGE>
00815013652512-16 12:57:57.547 F /disp:656:8303/ make post to autoconnect event from thread notifier! strDevImage == 15100000|1058|1
008150136645140|super|--|574D415A4139303734343136 uiDevState==1
00815013669712-16 12:57:57.550 F /disp:656:8303/ usb device with id == 15100000|1058|1140|super|--|574D415A4139303734343136 removed
008150136817from list excluded of autoconnect
00815013685112-16 12:57:57.551 F /gui:343:707/ localhost: received event PBT_DSP_EVT_HW_CONFIG_CHANGED, code = [100202]
00815013695912-16 12:57:57.555 F /gui:343:707/ localhost: sending [DspCmdUserGetHostHwInfo] request...
00815013705012-16 12:57:57.555 D /disp:656:a01f/ Processing command 'DspCmdUserGetHostHwInfo' 2051 (PJOC_SRV_GET_SRV_CONFIG)
```

J Raleigh|MacBook C02HW056DV31|D\Unallocated Clusters (P5 193845315 L5 193435675 CL 24179459 SO 144 FO 8150136464 LE 24)

**EnCase Screen Captures of a Parallels.log file in unallocated space from JRaleigh_RT2" aka "MacBook 340269NBATM
Dated 11/24/2012**

```
22650078d Reader> <PUDT_DISK_STORAGE>
2265010811-24 15:48:34.146 I /pvshostInfo:245:690b/ LOOKUP1 <26400000|1058|1140|high|--|574D415A4139303734343136> <My Book 1140>
22650228 <PUDT_DISK_STORAGE>
2265024911-24 15:48:34.182 F /disp:245:690b/ USB connected <26400000|1058|1140|high|--|574D415A4139303734343136> <My Book 1140>
22650369<PUDT_DISK_STORAGE>
2265038911-24 15:48:34.220 F /disp:245:690b/ make post to autoconnect event from thread notifier! strDevImage == 26400000|1058|1
22650509140|high|--|574D415A4139303734343136 uiDevState==1
2265056011-24 15:48:34.236 F /disp:245:690b/ make post to autoconnect event from thread notifier! strDevImage == 26400000|1058|1
22650680140|high|--|574D415A4139303734343136 uiDevState==1
2265073111-24 15:48:34.244 F /disp:245:690b/ usb device with id == 26400000|1058|1140|high|--|574D415A4139303734343136 removed f
22650851rom list excluded of autoconnect
2265088411-24 15:48:34.471 F /disp:245:690b/ On exit : dev_type = 15 dev_name = 26400000 event_code = 1
2265098311-24 15:48:38.467 F /disp:245:690b/ On enter : dev_type = 6 dev_name = IOMedia event_code = 0
2265108011-24 15:48:38.467 F /disp:245:690b/ Device change: host hardware info refreshing was skipped !
2265117611-24 15:48:38.482 F /disp:245:690b/ On exit : dev_type = 6 dev_name = IOMedia event_code = 0
2265127311-24 15:48:38.482 F /disp:245:690b/ On enter : dev_type = 15 dev_name = event_code = 0
2265136411-24 15:48:38.485 I /pvshostInfo:245:690b/ LOOKUP1 <24600000|05ac|8507|high|--|8JA6N2E5JDCLNA00> <Apple Built-in iSight
22651484> <PUDT_VIDEO>
2265149911-24 15:48:38.488 I /pvshostInfo:245:690b/ LOOKUP1 <6300000|05ac|0236|full|KM|Empty> <Apple Internal Keyboard / Trackpa
22651619d> <PUDT_KEYBOARD>
2265163811-24 15:48:38.489 I /pvshostInfo:245:690b/ LOOKUP1 <6500000|05ac|8242|low|--|Empty> <Apple IR Receiver> <PUDT_COMMUNICA
22651758TION>
2265176411-24 15:48:38.489 I /pvshostInfo:245:690b/ LOOKUP1 <6610000|05ac|8213|full|--|5C5948C71E36> <Apple Bluetooth USB Host C
22651884ontroller> <PUDT_BLUETOOTH>
2265191211-24 15:48:38.492 I /pvshostInfo:245:690b/ LOOKUP1 <26100000|05ac|8403|high|--|000000009833> <Apple Internal Memory Car
22652032d Reader> <PUDT_DISK_STORAGE>
2265206211-24 15:48:38.505 F /disp:245:690b/ USB disconnected <26400000|1058|1140|high|--|574D415A4139303734343136> <My Book 114
226521820> <PUDT_DISK_STORAGE>
2265220511-24 15:48:38.507 F /disp:245:690b/ make post to autoconnect event from thread notifier! strDevImage == 26400000|1058|1
22652325140|high|--|574D415A4139303734343136 uiDevState==0
2265237611-24 15:48:38.919 F /disp:245:690b/ On exit : dev_type = 15 dev_name = event_code = 0
2265246711-24 15:53:31.527 I /prl_time_machine_helper:245:307/ The Time Machine start up notification was received
2265257411-24 16:39:41.273 F /disp:245:6a03/ System events monitor: host going to sleep, prepare
2265266311-24 16:39:41.273 F /disp:245:6a03/ System events monitor: host going to sleep, done
```

J Raleigh|MacBook 340269NBATM|1 Macintosh HD|Macintosh HD|Library|Logs\parallels.log (P5 658973880 L5 658564240 CL 82320530 SO 358 FO 22651238 LE 1)

Toshiba External Hard Drive with NTFS Windows Partition

Looking at the screen capture below and referring to the most up to date database: <http://www.linux-usb.org/usb.ids> one can see that 0x048 (0480) is from Toshiba America Info. Systems, Inc. and 0x200 (0200) is an External Disk and 0x0 (00) is the release for that device. I located 1 entry for this device.

EnCase Screen Captures of a System.log file in unallocated space JRaleigh_LT1" aka "MacBook C02HW056DV31 from 10/15/2014

```
057007532882Oct 15 14:45:51 jrbmp Slack[576]: CGSCopyDisplayUUID: Invalid display 0x0424lead
057007532963Oct 15 14:45:51 jrbmp Slack[576]: CGSCopyDisplayUUID: Invalid display 0x78c59245
057007533044Oct 15 14:45:54 jrbmp kernel[0]: USBMSC Identifier (non-unique): 20140618002698F 0x480 0x200 0x0, 3
057007533144Oct 15 14:45:56 jrbmp Flux[431]: Display list confused, doing full reset.
057007533218Oct 15 14:45:59 jrbmp com.apple.kextd[19]: Can't create kext: invalid CFBundleVersion in identifier cache entry entry 34
0570075333389.
057007533341Oct 15 14:45:59 --- last message repeated 1 time ---
057007533394Oct 15 14:45:59 jrbmp com.apple.kextd[19]: kext com.github.osxfuse.filesystems.osxfusefs 204029000 is in exception list
057007533814, allowing to load
057007533533Oct 15 14:45:59 jrbmp kernel[0]: OSXFUSE: starting (version 2.4.2, Jun 6 2012, 13:39:25)
057007533623Oct 15 14:45:59 jrbmp ntfs-3g[5940]: Version 2010.10.2-mac external FUSE 27
057007533699Oct 15 14:45:59 jrbmp ntfs-3g[5940]: Mounted /dev/rdisklsl (Read-Write, label "TOSHIBA EXT", NTFS 3.1)
057007533802Oct 15 14:45:59 jrbmp ntfs-3g[5940]: Cmdline options: norecover,nfconv,auto_xattr,local,defer_permissions
057007533908Oct 15 14:45:59 jrbmp ntfs-3g[5940]: Mount options: auto_xattr,local,defer_permissions,allow_other,nonempty,relatime,fsn
057007534028ame=/dev/disklsl.volname=TOSHIBA EXT
057007534065Oct 15 14:45:59 jrbmp ntfs-3g[5940]: Ownership and permissions disabled, configuration type 1
057007534159Oct 15 14:46:00 jrbmp fseventsds[54]: could not open <>/Volumes/TOSHIBA EXT/.fsevents/fseventsds-uuid> (No such file or
057007534279directory)
057007534290Oct 15 14:46:00 jrbmp fseventsds[54]: log dir: /Volumes/TOSHIBA EXT/.fsevents getting new uuid: A1FED691-0C9E-450F-9E31-
0570075344104612FE188309
057007534423Oct 15 14:46:00 jrbmp com.apple.kextd[19]: Can't create kext: invalid CFBundleVersion in identifier cache entry entry 34
057007534539.
057007534546Oct 15 14:46:15 --- last message repeated 5 times ---
057007534600Oct 15 14:46:15 jrbmp diskarbitrationd[60]: unable to mount /dev/disklsl (status code 0xFFFFFFF).
057007534699Oct 15 14:46:15 jrbmp mds[44]: (Normal) Volume: volume:0x7fac28ad7000 ***** Bootstrapped Creating a default store:1
057007534819 SpotLoc:(null) SpotVerLoc:(null) occlude:0 /Volumes/TOSHIBA EXT
057007534840Oct 15 14:46:51 jrbmp Slack[576]: CGSCopyDisplayUUID: Invalid display 0x5b81c5c1
057007534965Oct 15 14:46:51 jrbmp Slack[576]: CGSCopyDisplayUUID: Invalid display 0x0424lead
```

J Raleigh|MacBook C02HW056DV31|D\Unallocated Clusters (PS 1420225374 LS 1419815734 CL 177476966 SO 113 FO 57007533169 LE 1)

IPad Devices & Findings

On the hard drive I was provided were Cellebrite extractions for 2 Apple iPad devices. Both devices were searched using Cellebrite's Physical Analyzer software. The search was negative for Malibu Media's works and for BitTorrent use and related activity.

1. iPad1_5.1-5.1.1_Physical_05-12-14_10-03-39
2. AppleDevice_AdvancedLogical_09-12-14_11-52-17